Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

П О Л О Ж Е Н И Е О Р Г А Н И З А Ц И И

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

Положение об организации парольной защиты в ФГБОУ ВО «ИРНИТУ»

ОРИГИНАЛ

Содержание

УТВЕРЖДЕНО
Приказом ректора
(чем) (должность)

от «01» октября 2025 г. № 687-О
(дата)

П О Л О Ж Е Н И Е О Р Г А Н И З А Ц И И

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

Положение об организации парольной защиты в ФГБОУ ВО «ИРНИТУ» Введено впервые

1 Область применения

1.1 Настоящее положение разработано в целях установления порядка процессов генерации, смены и прекращения действия паролей в информационных системах и системах обработки информации ФГБОУ ВО «ИРНИТУ».

1.2 Требования данного положения распространяются на всех работников и обучающихся всех форм обучения, абитуриентов и внешних слушателей ФГБОУ ВО «ИРНИТУ».

2 Нормативные ссылки

Настоящее положение разработано в соответствии и содержит ссылки на следующие нормативные документы:

Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации.

Приказ ФСТЭК России от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 28.08.2024) "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".

Методические рекомендации ФСТЭК: "Методический документ. Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021), "Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (Выписка) (утв. ФСТЭК РФ 15.02.2008).

Национальные стандарты Российской Федерации: ГОСТ Р 53114-2008 "Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения", ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования".

Устав Иркутского национального исследовательского технического университета.

СТО 001 Система менеджмента качества. Общие требования к оформлению документов СМК.

СТО 002 Система менеджмента качества. Порядок управления документированной информацией (документами) СМК.

3 Термины, определения и сокращения

3.1 В настоящем положении применены следующие термины с соответствующими определениями:

Active Directory – это база данных (каталог) и набор служб, которые позволяют администраторам управлять пользователями, компьютерами, группами, политиками безопасности и другими сетевыми ресурсами в доменной сети с одного сервера.

Авторизация – это процесс проверки прав и разрешений уже аутентифицированного пользователя на выполнение определенных действий или доступ к ресурсам.

Аутентификация – это процесс проверки и подтверждения подлинности пользователя или системы.

Базовая Информационная Обслуживающая Система – это базовая система ввода-вывода, встроенное в материнскую плату компьютера низкоуровневое программное обеспечение, которое является мостом между аппаратным обеспечением (железом) и операционной системой.

Информационная система – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием вычислительной техники.

Логин – это уникальное имя пользователя, которое используется для идентификации и авторизации в информационных системах, в компьютерной системе, приложении или сети.

Локальная Вычислительная Сеть – это группа компьютеров и других устройств (например, принтеров, серверов), соединенных между собой с помощью кабелей или беспроводных технологий в ограниченной географической зоне (такой как здание, офис, кампус университета или даже квартира) и предназначенная для совместного использования ресурсов, данных и связи между пользователями.

Пароль – комбинация цифр, букв и других знаков для получения доступа к различным данным, принадлежащая субъекту доступа, который является его (субъекта) секретом.

Политика парольной защиты – это набор формальных правил и требований, разработанный для повышения безопасности информационных систем путем принудительного использования стойких (сложных) паролей и управления их жизненным циклом.

Политика парольной защиты домена – это централизованно управляемый наборных правил, регламентирующих структуру, периодичность смены и историю паролей учетных записей, а также реакцию системы на многократные неудачные попытки входа, с целью повышения общей кибербезопасности сетевой инфраструктуры.

Пользователь – физическое лицо (работник, обучающийся, абитуриент, школьник или внешний пользователь), использующее ресурсы информационной системы ФГБОУ ВО «ИРНИТУ» для выполнения задач, связанных с образовательной, научной, административной или иной деятельностью университета.

Пользователь домена – это учетная запись, созданная в домене Active Directory, которая позволяет пользователю аутентифицироваться на контроллерах домена и получать доступ к сетевым ресурсам, таким как компьютеры, принтеры, файловые хранилища и приложения, в соответствии с назначенными правами и разрешениями. Для обеспечения безопасности такая учетная запись подчиняется политике парольной защиты домена.

Право на доступ – совокупность правил, регламентирующих порядок и условия доступа пользователя ИС к ее ресурсам.

Привилегия на доступ – исключительное право на доступ к ресурсам информационной системы.

Система менеджмента качества – часть системы менеджмента применительно к качеству.

Стандарт организации – нормативный документ по стандартизации, разработанный, как

правило, на основе согласия, характеризующегося отсутствием возражений по существенным вопросам у большинства заинтересованных сторон, устанавливающий комплекс норм, правил, требований к различным видам деятельности университета или их результатам и утвержденный приказом руководства университета.

3.2 В настоящем положении используются следующие сокращения:

АРМ – Автоматизированное рабочее место;

БИОС – Базовая Информационная Обслуживающая Система;

ИС – информационная система;

ЛВС – Локальная вычислительная сеть;

СМК – система менеджмента качества;

СТО – стандарт организации;

ФГБОУ ВО «ИРНИТУ» – Федеральное государственное бюджетное образовательное учреждение высшего образования «Иркутский национальный исследовательский технический университет».

4 Ответственность

4.1 Ответственность за разработку, пересмотр, идентификацию внесенных изменений в данное положение возложена на начальника отдела информационной безопасности и документооборота ФГБОУ ВО «ИРНИТУ».

4.2 Разработчик настоящего положения осуществляет периодическую проверку (пересмотр) данного положения в установленном порядке согласно СТО 002 Система менеджмента качества. Порядок управления документированной информацией (документами) СМК.

4.3 Ответственность за выполнение требований настоящего положения возлагается на всех пользователей информационных систем ФГБОУ ВО «ИРНИТУ», являющихся владельцами учетных записей.

5 Общие положения

5.1 Настоящее положение регламентирует установку, смену и прекращение действия паролей, блокировку учетных записей пользователей в ЛВС.

5.2 Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах информационных систем, контроль за действиями пользователей информационных систем при работе с паролями возлагается на пользователей и администраторов соответствующих информационных систем.

5.3 Все учетные записи (включая системные, служебные и учетные записи пользователей и администраторов) в системном и прикладном программном обеспечении, а также системы и средства защиты информации (включая доступ к БИОС и к управлению персональными межсетевыми экранами и антивирусным программным обеспечением) должны быть защищены стойкими методами аутентификации.

5.4 Пароль представляет собой комбинацию, известную только пользователю, предназначенную для аутентификации пользователя в операционной системе автоматизированного рабочего места и в ЛВС. Пароль является средством защиты от несанкционированного доступа к информации или средствам ее обработки, хранения и передачи.

5.5 Настоящее Положение предназначено для применения всеми пользователями информационными системами во всех его структурных подразделениях, использующих средства информатизации и информационные системы ФГБОУ ВО «ИРНИТУ».

5.6 Все действующие Пользователи должны быть ознакомлены с настоящим Положением в установленном порядке.

5.7 Работники должны быть ознакомлены с настоящим Положением Управлением по работе с персоналом при приеме на работу (до подписания трудового договора).

5.8 Обучающиеся должны быть ознакомлены с настоящим Положением работниками дирекций институтов.

5.9 Абитуриенты поступающие в ФГБОУ ВО «ИРНИТУ» должны быть ознакомлены с настоящим Положением работниками управления по работе с абитуриентами.

5.10Настоящее положение применимо к следующим группам учетных записей:

a) Сервисные учетные записи — Учетные записи, используемые не людьми, а приложениями, службами или системами для взаимодействия друг с другом и доступа к ресурсам.

b) Пользовательские учетные записи — Стандартные учетные записи для рядовых сотрудников ФГБОУ ВО «ИРНИТУ». Они предоставляют доступ к необходимым для повседневной работы ресурсам: почте, корпоративным системам, сетевым папкам и т.д.

c) Студенческие учетные записи — Учетные записи, предназначенные для студентов ФГБОУ ВО «ИРНИТУ». Обычно имеют доступ к образовательным ресурсам, библиотечным системам, Wi-Fi и компьютерным классам.

d) Учетные записи слушателей — Учетные записи для временных пользователей: стажеров, курсов повышения квалификации, школьников, гостей. Часто имеют ограниченный срок действия и самый минимальный набор прав доступа.

e) Инженерные учетные записи — Учетные записи для технических специалистов (инженеров, разработчиков, аналитиков). Обычно имеют повышенные привилегии для настройки оборудования, установки ПО, управления специализированными системами, но не для полного администрирования сети.

f) Административные учетные записи — Учетные записи с максимальными привилегиями (например, администратор домена, root). Используются для управления критической ИТ-инфраструктурой: серверами, сетевым оборудованием, системами безопасности. К ним применяются самые строгие политики паролей и учета.

5.11Ответственные за распределение по группам учетных записей являются сотрудники отдела информационной инфраструктуры управления информатизации.

6 Требования к паролям

6.1 Требования к паролю могут зависеть от группы, к которой принадлежит пользователь, а также от требований к доступу сервиса, к которому получает доступ пользователь.

6.2 Личные пароли пользователей для доступа к информационным системам и ресурсам ФГБОУ ВО «ИРНИТУ», а также пароли, применяемые для работы во внешних системах от имени ФГБОУ ВО «ИРНИТУ», должны формироваться и распределяться с учетом общих требований.

6.3 Требования, относящиеся ко всем группам учетных записей:

a) идентификаторы пользователей и их пароли должны быть уникальными для каждого пользователя;

b) в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры. Рекомендуется использовать в парольной фразе специальные символы (@, #, $, &, *, % и т.п.);

c) пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, важные для пользователя даты, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, АС, USER и т.п.);

d) пароли должны генерироваться автоматически и после ввода администратором учетной записи передаваться пользователям;

e) пароли должны держаться в тайне, то есть не должны сообщаться другим людям, не должны вставляться в тексты программ, и не должны записываться на бумагу;

f) при смене пароля новое значение должно отличаться от предыдущего не менее чем

в 3 позициях для предотвращения использования того же самого или угадываемого пароля;

g) учетные данные пользователей должны быть заблокированы после 10 неудачных попыток входа в систему на срок 20 минут. Все случаи неверно введенных паролей должны быть записаны в системный журнал, в целях определения и расследования инцидента информационной безопасности;

h) сеансы работы пользователей с АРМ и сетевых соединений с сервером должны блокироваться после 15 минут отсутствия активности. Для возобновления сеанса должен снова требоваться ввод пароля.

6.4 Требования, относящиеся к Пользовательские учетные записи, Студенческие учетные записи, Учетные записи слушателей:

a) пароли должны состоять как минимум из 10 символов (не должны быть именами или известными фразами);

b) пароли должны меняться не реже, чем каждые 90 дней.

6.5 Специализированные требования, относящиеся к сервисным учетным записям:

a) пароли должны состоять как минимум из 25 символов (не должны быть именами или известными фразами);

b) пароли не имеют срока обновления.

6.6 Требования, относящиеся к инженерным учетным записям:

a) пароли должны состоять как минимум из 12 символов (не должны быть именами или известными фразами);

b) пароли должны меняться не реже, чем каждые 60 дней.

6.7 Требования, относящиеся к административным учетным записям:

a) пароли должны состоять как минимум из 16 символов (не должны быть именами или известными фразами);

b) пароли должны меняться не реже, чем каждые 30 дней.

6.8 Пользователи должны быть ознакомлены с перечисленными выше требованиями и нести ответственность за разглашение парольной информации, а также за использование паролей, не соответствующих данным требованиям;

6.9 Пользователи при первом входе в информационные системы ФГБОУ ВО «ИРНИТУ» обязаны осуществить смену выданного временного пароля администратором информационной системы на свой удовлетворяющий требованиям настоящего Положения;

6.10 Для генерации «стойких» паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления посторонних лиц с паролями работников подразделений.

6.11 В случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п., а также при наличии технологической необходимости использования имен и паролей некоторых пользователей в их отсутствие, такие пользователи обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение администратору информационной безопасности или руководителю своего подразделения. Опечатанные конверты с паролями пользователей должны храниться в недоступном для остальных пользователей месте. Для опечатывания конвертов должны применяться личные печати владельцев паролей (при их наличии), либо печать администратора информационной безопасности или ректора ФГБОУ ВО «ИРНИТУ».

7 Требования к парольной политике домена

7.1 В рамках домена ФГБОУ ВО «ИРНИТУ» должны использоваться централизованные политики парольной защиты, реализуемые средствами контроллера домена на основе Active Directory с применением групповых политик.

7.2 Все компьютеры ФГБОУ ВО «ИРНИТУ» должны быть подключены к домену Active Directory согласно приказу 256-О от 11 апреля 2022г.

7.3 Требования, предъявляемые для паролей доменных пользователей, являются обязательными для применения всеми работниками ФГБОУ ВО «ИРНИТУ» и включают в себя:

a) идентификаторы пользователей и их пароли должны быть уникальными для каждого пользователя;

b) пароли должны состоять как минимум из 10 символов (не должны быть именами или известными фразами);

c) в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры. Рекомендуется использовать в парольной фразе специальные символы (@, #, $, &, *, % и т.п.);

d) пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, логины, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, АС, USER и т.п.);

e) пароли должны меняться не реже, чем каждые 90 дней;

f) пароли не должны меняться чаще, чем каждые 5 дней;

g) при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 символах;

h) учетные данные пользователей должны быть заблокированы после 10 неудачных попыток входа в систему на срок 20 минут. Все случаи неверно введенных паролей должны быть записаны в системный журнал, в целях определения и расследования инцидента информационной безопасности;

i) сеансы работы пользователей с АРМ и сетевых соединений с сервером должны блокироваться после пятнадцатиминутной неактивности (или другого согласованного периода). Для возобновления сеанса должен снова требоваться ввод пароля;

j) новый пароль должен отличаться от 20 предыдущих;

k) напоминание о необходимости смены пароля не ЗАРАНЕЕ чем за 7 дней до истечения срока действия пароля.

8 Смена паролей

8.1 Плановая смена паролей пользователей должна проводиться регулярно, не реже 90 дней. Внеплановая смена личного пароля, блокировка или удаление учетной записи работника ФГБОУ ВО «ИРНИТУ» в случае прекращения его полномочий (увольнение, переход в другое подразделение и т.д.) должна производиться уполномоченными работниками – немедленно с принудительным завершения сеанса работы пользователя с информационными системами.

8.2 В случае компрометации личного пароля пользователя должны быть немедленно предприняты меры по внеплановой смене паролей в зависимости от полномочий владельца скомпрометированного пароля.

8.3 Хранение пользователем значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у начальника отдела информационной безопасности или руководителя подразделения в опечатанном личной печатью конверте (возможно вместе с персональными ключевыми носителями).

Приложение 1 Лист согласования положения об организации парольной защиты в ФГБОУ ВО «ИРНИТУ»
(обязательное)

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Дата	Подпись
Проректор по кампусному и корпоративному управлению	С.С. Аносов	19.09.2025	
Проректор по международной деятельности	С.С. Быков	19.09.25	
Проректор по научной работе	А.М. Кононов	19.09.25	
Советник ректора	Е.Г. Можаева	19.08.25	
Проректор по учебной работе	В.В. Смирнов	19.09.2025	
Проректор по молодежной политике	Д.Н. Лобанова	19.09.2025г	
Начальник управления по работе с персоналом и обучающимися	Т.Ю. Гуруленко	19.09.2025	
Начальник управления планирования, бухгалтерского учета и аудита	Н.Б. Максимова	19.08.25	
Начальник управления по дополнительному образованию и социальной работе	Б.Б. Пономарев	19.09.2025	
Начальник управления информатизации	А.Р. Захарченко	19.09.2025	
Руководитель юридической службы	О.Л. Пенизева	19.09.2025	
Начальник отдела мониторинга и менеджмента качества	О.С. Артемова	19.09.2025	
Начальник управления по работе с абитуриентами	Н.А. Вострикова	19.09.2025	

РАЗРАБОТАНО:

Начальник отдела информационной безопасности и документооборота	Д.Д. Денисевич	19.09.2025	

Приложение 2 Лист регистрации изменений положения об организации парольной защиты в ФГБОУ ВО «ИРНИТУ»

(обязательное)

Порядковый номер изменения	**Основание (№ приказа, дата)**	**Дата введения изменения**	**Изменения внёс**	
			Фамилия, инициалы	**Подпись вносившего изменения, дата внесения**
1	2	3	4	5

Приложение 3 Лист ознакомления с положением об организации парольной защиты в ФГБОУ ВО «ИРНИТУ»
(обязательное)

№	И.О. Фамилия	Должность	Дата	Подпись